

A CONCEPTUAL FRAMEWORK FOR BIOSECURITY LEVELS

Jennifer Gaudioso, Ph.D.

Sandia National Laboratories, P.O. Box 5800, MS 1373, Albuquerque, NM 87185

Phone: (505) 284-9489, email: jmgaudi@sandia.gov

Reynolds M. Salerno, Ph. D.

Sandia National Laboratories, P.O. Box 5800, MS 1373, Albuquerque, NM 87185

Phone: (505) 844-8971, email: rmsaler@sandia.gov

Presented at:

“BTR 2004: Unified Science and Technology for
Reducing Biological Threats and Countering Terrorism,”

University of New Mexico, Albuquerque, NM, 18-19 March 2004

ABSTRACT:

There is a growing awareness in the microbiological research and policy communities of the need to increase the protection of dangerous pathogens from theft and sabotage. However, existing security literature and regulatory requirements do not present a comprehensive approach or clear model for biosecurity, nor do they wholly recognize the operational issues within laboratory environments. To help address these issues, the concept of Biosecurity Levels should be developed. Biosecurity Levels would have increasing levels of security protections depending on the attractiveness of the pathogens to adversaries. This paper proposes a preliminary framework for assessing Biosecurity Level requirements and provides examples addressing specific biological materials.

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under contract DE-AC04-94AL85000.

INTRODUCTION

Recent events, such as the 2001 anthrax mailings, Aum Shinrikyo's attempts in the mid-1990s to disseminate anthrax and botulinum toxin, and reported al Qaeda interest in biological weapons (BW), have catalyzed a growing sense of urgency concerning potential BW terrorism and proliferation. As a result, there is broad agreement that those biological agents and toxins that could be used as a terrorist weapon warrant increased control and oversight. However, the security of such agents and toxins is just beginning to be addressed. The US government has passed several relevant laws,¹ the National Academies have published a report with multiple recommendations for research oversight,² and USDA's Office of Inspector General has published a report arguing for increased physical security for biological agents.³

There is no doubt that the application of biosecurity – the protection of dangerous pathogens and toxins from theft and sabotage – will never be perfect or foolproof, and that biosecurity only addresses a very small part of the BW terrorism and proliferation problem. The nature of dangerous pathogens is such that a person could steal a very small amount of material from a legitimate research or diagnostic facility and grow, process, and deploy that material as a weapon with commercially available equipment. Moreover, biotechnology has advanced so that virulent and viable organisms can be constructed synthetically or from genetically engineering a chimera from two relatively harmless agents.⁴ In other words, an individual with malevolent intent need not have or gain access to a known dangerous pathogen or toxin to be able to perpetrate bioterrorism.

Nevertheless, it is evident that the serious consequences associated with the use of biological weapons justify improving control and oversight over biological material that could be deployed as a terrorist weapon. It is now essential and appropriate to establish biosecurity systems, practices, and procedures that deter and detect the malicious diversion of these biological materials. However, it is critically important to strike an appropriate balance between protection of biological material that could be used in a biological weapon and preservation of an environment that promotes legitimate and lifesaving microbiological research.⁵

Several unique aspects of biological materials should be considered when designing a biosecurity system. First, in spite of their potential use for hostile purposes, all biological agents are valuable for a variety of legitimate, defensive, and peaceful commercial, medical, and research applications. This dual-use characteristic makes it extremely difficult to distinguish between legitimate and illegitimate laboratory use of these agents. Second, biological agents can be isolated from nature and are found in a variety of biomedical research institutes, clinical facilities, biotechnology industries, and culture collections around the world.* Although due diligence and prudent stewardship of material is necessary, higher levels of biosecurity are only warranted when material is difficult to obtain—not when it is ubiquitous. Third, biological agents are living, self-replicating organisms. These organisms and their by-products (toxins) can vary in quantity and quality over the course of legitimate research activities by growing, dying, and mutating. Therefore, knowing the exact quantity of organisms or molecules of an agent or toxin in a laboratory is not achievable. Fourth, within legitimate facilities, biological agents can be isolated from a number of process streams. They can be found in Petri dishes, cell cultures, environmental samples, clinical specimens, infected animals, and animal carcasses, as well as stored in refrigerated or freeze-dried forms. This wide distribution of the assets that need to be secured makes safeguarding all of the material extremely difficult. Finally, biological agents cannot be detected with available stand-off technologies. Therefore, detecting someone who is illegally removing biological material is almost impossible.

In order to design an appropriate security system, which considers all of the unique challenges associated with protecting pathogens, a methodology that aims to establish clear objectives for the biosecurity system should be used. In particular, the biosecurity system designers should employ a risk management approach

* The one exception is the Variola major virus, the causative agent of smallpox, which has been globally eradicated. The two official repositories are the CDC, Atlanta (USA) and the State Research Institute for Virology and Biotechnology, Koltsovo (Russia).

that 1) establishes which assets should be protected against which threats, and 2) ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportionate to the potential consequence of the theft of that asset.⁶ This risk-based, graded approach helps ensure that assets, whose loss would have the most serious impact on national security, or the health, safety, and well being of the public or environment, are secured with the resources necessary to achieve the highest level of protection. At the same time, this approach helps ensure that limited resources are not spent securing material that would not be attractive to adversaries.

CURRENT US BIOSECURITY REGULATIONS

The current US biosecurity regulatory environment is based on two laws, the USA PATRIOT Act and the Bioterrorism Preparedness Act, which aim to improve the protection of “select” agents and toxins. Three Codes of Federal Regulations (42 CFR 73, 7 CFR 331, and 9 CFR 121, or collectively “CFR”) establish lists of agents and toxins that pose a threat to humans, animals, or plants, and require any laboratory that possesses any one of these 80+ listed agents or toxins to enforce and adhere to a series of specific security measures. The security requirements include facility registration, designation of a responsible official, background checks for individuals with access to the listed agents, biosecurity plans, agent transfer rules, safety and security training and inspections, notification following identification, theft, loss, or release of a listed agent, record maintenance, and restrictions on some types of experiments.⁷

Recently, many researchers and laboratories have decided to discontinue or not pursue research on regulated biological agents, rather than implement the new security regulations and bear the associated financial burden. According to the supplementary information published in December 2002 in 42 CFR 73, the Centers for Disease Control and Prevention (CDC) expected 817 entities to register under the new select agent rule. Instead, only 323 facilities are now registered with the CDC, indicating that many institutions have discontinued their work with select agents.⁸ Security regulations that induce such a negative response in the research community will stifle valuable public health and biodefense research, further compromising our ability to respond to bioterrorism and infectious disease outbreaks.

Many people in the US microbiological research community perceive the CFR as an inappropriate impediment to important research. We believe that this perception could be changed if an agent-based risk-management methodology were applied to biosecurity. Such a graded approach would improve the likelihood that scarce security resources would be allocated specifically to those biological materials judged to be at greatest risk for theft or sabotage. Unfortunately, the current US regulations apply a black-or-white standard to biosecurity: either an agent is on the regulated list and requires security or it is not on the list and needs no security. *Coccidioides immitis*, *Bacillus anthracis*, and Variola major virus are all select agents, legally subject to the same security standards. We contend that all CFR-listed agents and toxins are not equally vulnerable to BW proliferation, and therefore do not require the same level of protection. Investments in security, especially if these resources come out of limited research budgets, should be focused on those agents that are most attractive to adversaries interested in diverting materials that could be used to build biological weapons.

BIO SAFETY AS A MODEL FOR BIOSECURITY

Microbiological laboratories regularly work with biological agents that can cause human disease and, as a result, laboratory-acquired infections have occurred since the beginning of such research. Biosafety aims to protect the laboratory workers and the environment from accidental exposure to hazardous biological agents. But prior to 1984, there were no uniform standards for applying specific biosafety techniques and equipment to certain types of research. To provide guidance and ensure consistency, the CDC and the National Institutes of Health (NIH) developed the concept of Biosafety Levels and published guidelines for implementing them in a manual entitled, “Biosafety in Microbiological and Biomedical Laboratories,” also known as the BMBL. The BMBL, which is now in its fourth edition, provides a framework for researchers to determine the appropriate Biosafety Level for their work based on the pathogen and the experiment; it then details the suggested safety practices for each level.

The BMBL recommends various degrees of laboratory containment, or safe methods of managing infec-

tious materials in a laboratory setting to achieve appropriate biosafety.⁹ There are three components that work together to establish containment: laboratory practices and techniques, safety equipment (primary barriers), and facility design and construction (secondary barriers). The BMBL describes four Biosafety Levels that represent a graded application of barriers, practices, and techniques. The BMBL recommends Biosafety Levels based on the hazard of the agent and the experiment to laboratory workers and the environment. The BMBL also stresses that a thorough risk assessment should be completed for any laboratory activity involving potentially infectious material. The goal of this biosafety risk assessment is to judge the probability that disease may occur as well as the consequences of that disease occurring. The results of such an assessment, taken together with the recommendations in BMBL agent summary statements, should guide the selection of an appropriate Biosafety Level to conduct the work.

Over time, the microbiological research community has widely recognized and embraced the benefits of laboratory biosafety standards as detailed in the BMBL. The US-developed guidelines have become the basis of international biosafety standards, increasing safety worldwide.¹⁰

FRAMEWORK FOR BIOSECURITY LEVELS

In contrast to biosafety, existing security literature and regulatory requirements do not present a comprehensive approach or clear model for biosecurity, nor do they wholly recognize the operational issues within bioscience laboratory environments. To help address these issues, we recommend the development of the concept of Biosecurity Levels. Similar to Biosafety Levels, Biosecurity Levels should have increasing levels of protection as the nature of the pathogen or experiment changes, but the focus should be on protecting the pathogen rather than the worker or the environment.

Agents would be placed in a Biosecurity Level based upon their risk of being stolen and used maliciously as a biological weapon. This risk entails both the probability and the consequences of use. We associate the probability of use with the ease or difficulty involved in deploying the agent as a weapon, or its weaponization potential, because we believe that the easier the agent is to use as an effective weapon, the more likely it is that an adversary will choose it as an agent of biological terrorism. An analysis of the probability of use should include such factors as the availability of a suitable strain, ease of production (an appropriate quantity in an appropriate form), modes of dissemination, hardness of the agent (both in the laboratory and after deployment), and the availability and level of knowledge required to use the agent as a weapon. An examination of the potential consequences of use should necessarily involve factors such as infectious dose, incubation period, pathogenicity, availability of preventive measures and/or post-exposure treatments, and modes and ease of transmission.

In an effort to acknowledge the possibility of bioterrorism, a CDC Strategic Planning Workgroup¹¹ that met in 1999 evaluated the public health consequences of some agents. They divided agents into three categories: A, B, and C agents. It was determined that Category A agents should receive the highest levels of public health preparedness; public health deficiencies related to Category B agents should be corrected; and Category C agents should be monitored because they were considered “emerging” agents. While useful, this categorization excluded those agents that represent a threat to animal and plant health. An outbreak of Foot and Mouth Disease would clearly have a devastating impact on the US economy. Moreover, this evaluation focused almost exclusively on the consequences to public health, and did not adequately reflect an evaluation of the ease or difficulty in deploying the agents as weapons. A few of the Category B agents, such as the *Brucella* species and *Coxiella burnetii*, may present a significant biological weapons threat.

Weighing both the probability and consequences of the malicious use of an agent as a weapon would allow the selection of a Biosecurity Level that is proportional to the risk of the agent being used as a weapon. We contend that the security risk that an agent presents is not necessarily the same as the safety risk. Hence, Biosecurity Levels should not be the same as Biosafety Levels. For instance, there are some agents that are used in BSL-2 facilities (e.g. *Bacillus anthracis*, *Yersinia pestis*) that arguably are more attractive to adversaries, and should be better protected, than some BSL-3 agents (e.g. West Nile Virus, Vesicular Stomatitis Virus).

We foresee that the overwhelming majority of biological agents would be evaluated as a minimal security risk and, thus, assigned to a Biosecurity Level that recommends minimal protections. The highest level of security would be required for only a very few agents, including those that have been eradicated from nature. Biosecurity Levels would recommend higher security than that currently mandated by federal regulations for those very few agents that represent a true weapons risk, and lower levels of security for those agents that would be considered less attractive to adversaries who are interested in pursuing bioterrorism or BW proliferation.

EXAMPLE AGENT RISK ASSESSMENTS

Perhaps the best way to understand why different biological agents warrant different degrees of security is to analyze a few examples. Qualitative, and not comprehensive, risk assessments for selected examples are described below. By analyzing the ease or difficulty of deploying the agent as a weapon (its weaponization potential or probability of use) and the public and/or agricultural health impacts of using the agent as a weapon (consequences), we demonstrate that not all agents present an equal risk for BW terrorism or proliferation and, thus, not all agents are equally attractive to adversaries intent on stealing them from legitimate laboratories. This type of analysis helps to justify a graded, agent-based approach to biosecurity.

Mycobacterium leprae

Consequences of Use: *M. leprae* is the causative agent for leprosy. It is a Gram positive, rod-shaped bacterium that does not form spores. This agent is not highly virulent: most people who are exposed to it do not develop leprosy.¹² For those individuals who contract the disease, the majority of patients recover without specific treatment; the remaining patients can be cured through a multi-drug treatment regiment.¹³ *M. leprae* has an incubation period of two to twenty years.¹⁴ The person-to-person transmission mechanisms are not fully understood, but *M. leprae* is not highly contagious.

Probability of Use: Production of any quantity of *M. leprae* would be a significant challenge since this agent has never been successfully grown in artificial media or human tissue cultures. *M. leprae* is a very slow growing organism with a generation time of up to 30 days.¹⁴ *M. leprae* does not form spores so it is not expected to be environmentally hardy.

Based on our analysis, we would consider *M. leprae* to have both low consequence and low probability of use as a weapon.

Coccidioides immitis

Consequences of Use: *C. immitis* is a fungus that is pathogenic to humans and animals. Infection may cause coccidioidomycosis (also known as Valley Fever or Desert Fever). Coccidioidomycosis is not contagious and there is a high natural immunity in areas where it is endemic. Infection is usually asymptomatic; 30 – 40% of the infected become ill.¹⁵ Most cases resolve without any treatment. Since only five to ten out of every 1,000 persons infected might develop a life-threatening infection, Deresinski, a Coccidioides researcher, concludes “that this fungus is not an outstanding candidate as a weapon of war or of bioterrorism.”¹⁵ *C. immitis* is not included on the CDC Category A, B, or C lists of potential biological threats, but it is a select agent.

Probability of Use: To work with this agent requires technological knowledge. Biosafety Level 3 is recommended for all activities with cultures and for processing soil likely to contain infectious *C. immitis*.¹⁶ Coccidioidomycosis is the tenth most common laboratory infection. The disease is endemic to arid and semi-arid areas of the Western Hemisphere. Because of its wide distribution, the fungus is easy to procure but testing must be done to identify a virulent strain. It is straightforward to grow colonies and induce spore formation.¹⁷ *C. immitis* is not known to have been weaponized by a state program.

Based on our analysis, we would consider *C. immitis* to have minor to moderate consequence and moderate probability of use as a weapon.

Bacillus anthracis

Consequences of Use: *B. anthracis* are Gram-positive, rod-shaped bacteria that form spores. Aerosolized

B. anthracis causes pulmonary anthrax, which has a high fatality rate (>60%).¹⁸ Diagnosis during the early stages of infection is difficult; anthrax initially presents as a nonspecific, flu-like illness. Pre-event vaccination and early post-event antibiotic treatment can prevent infection. A relatively high infectious dose (LD₅₀ = 2,500 – 55,000 spores) is required to cause infection¹⁹ and anthrax is not transmissible from person to person. *B. anthracis* is listed as a CDC Category A agent.

Probability of Use: *B. anthracis* has been weaponized by many former national programs, including the United States, Great Britain, the Soviet Union, and Iraq, and it has been used for bioterrorism. Most work with *B. anthracis* can safely be done at Biosafety Level 2. *B. anthracis* is endemic to much of the world but there are many weakly virulent strains, so strain-typing is required. This agent grows readily on all common laboratory media and easily forms spores.¹⁹ The spores are exceptionally stable in storage and in the environment. There are differences of opinion as to the ease of aerosolizing the spores. However, the 2001 anthrax letters and a recent Canadian study of an agricultural spraying of a related agent²⁰ seem to indicate that creating suitable *Bacillus* aerosols is not particularly challenging.

Based on our analysis, we would consider *B. anthracis* to have moderate to high consequence and of relatively high probability of use as a weapon.

Variola major virus

Consequences of Use: The infectious dose for Variola major to cause smallpox is unknown but believed to be only a few virions. A vaccine is available and offers high protection when administered up to twenty-four hours post-exposure.²¹ Treatment is otherwise mostly limited to supportive care. Since the eradication of smallpox, there are relatively few people who have been vaccinated against it, providing almost universal susceptibility in the general population to the disease. Previous epidemics have resulted in a 30% fatality rate. This fatality rate may be higher in naïve populations; smallpox epidemics among the American Indians resulted in a greater than 50% fatality rate.²¹ Smallpox is contagious but there is controversy about whether the spread of infection is limited to close contact. Further, the carrier is most infectious while suffering from fever and pox rash. There is a distinct possibility of genetically engineering Variola virus to be more virulent. Genetic engineering resulting in increased virulence has been demonstrated for other orthopox viruses²² and the Soviets may have been working on increasing the virulence of Variola major virus.²³

Probability of Use: Variola major was weaponized by the Soviet Union. Variola major belongs to the class of orthopox viruses. These viruses are very stable in aerosols,²⁴ displaying significant viability for several hours over a wide range of temperatures and relative humidity. The viruses remain viable for up to two days after release before becoming fully inactivated. Variola virus has been eradicated from nature and exists in only two official repositories, so obtaining the virus should be extremely difficult.

Based on our analysis, we would consider Variola major to have high consequence and moderate probability.

PROPOSED BIOSECURITY LEVELS

These qualitative assessments illustrate that not all agents are equally likely to be targeted for diversion by an adversary. The choice of agents for our analysis also demonstrates that, even for CFR-listed agents and toxins, there is considerable variation in weaponization potential. This paper suggests four Biosecurity Levels replace the two de-facto levels (protected or not) established by the CFR.

Low Risk Pathogens and Toxins (LRPT): The consequence of the use of any of these agents as a weapon is considered low.

We recommend classifying *M. leprae* as a LRPT.

Securing a LRPT would be done at a “low security risk level” and would entail basic protection measures

that are commonly part of good bioscience business practices. The doors should be locked in unattended laboratories. The principal investigator should be aware of the work and people in his/her laboratory. Laboratory notebooks should document the stocks and use of agents.

Moderate Risk Pathogens and Toxins (MRPT): These agents are relatively difficult to deploy as a weapon and their use as a weapon would have localized consequences with low to moderate casualties and/or economic damage.

We recommend classifying *C. immitis* as a MRPT.

Securing a MRPT would be done at a “moderate security risk level” and would include an appropriate increase in protection, but these measures should not be difficult for the biological research and public health communities to implement. For instance, laboratories where MRPT are used or stored should have access controls (e.g. controlled keys) that provide reasonable assurance that only authorized personnel can enter. A basic personnel suitability check should be completed for all those who enter the controlled area. Materials should be accounted for and inventoried in databases that are consistent across the facility.

High Risk Pathogens and Toxins (HRPT): These agents are not particularly difficult to deploy as a weapon and their use as a weapon could have national or international consequences, causing moderate to high casualties and/or economic damage.

We recommend classifying *B. anthracis* as a HRPT.

These agents should be secured at a “high security risk level” which would require relatively stringent security measures. Access should be strictly controlled with electronic systems. Personnel screening should include more detailed background investigations than those conducted on individuals who only work with MRPT. Accountability records should be maintained, and material transfers should be pre-approved and require a continuous chain of custody. Information about the security of these agents should be protected as well. A Biosecurity Officer should oversee the implementation of appropriate biosecurity measures.

Extreme Risk Pathogens and Toxins (ERPT): These agents would normally be classified as HRPT, except for the fact that they are not found in nature. This could include genetically engineered agents, if they were suspected of representing a high-risk pathogen or toxin.

The analysis would place *Variola major* in the HRPT category, except that it has been eradicated from nature. Thus, we recommend classifying *Variola major* as an ERPT.

Protection measures taken at the “extreme risk level” would be the most restrictive and it is anticipated that very few facilities would have the need or capability to meet these security guidelines. Two- or three-level electronic access controls should be imposed, and strict personnel suitability background checks should be conducted on all persons who enter the laboratory. Accountability records should be maintained, and material transfers should be pre-approved and require a continuous chain of custody. Information about the security of these agents should be protected as well. A local guard force should be able to respond to intrusions. Two authorized individuals should be required for access to stocks. A Biosecurity Officer should oversee the implementation of appropriate biosecurity measures.

Table 1 provides more detail on the concept of Biosecurity Levels by providing examples of graded implementation of the components of a biosecurity program. An effective and efficient biosecurity program should include physical security, personnel security, information security, material control and accountability, material transfer security, and biosecurity program management. As detailed in Table 1, a graded implementation of these six components of biosecurity would work together to establish an appropriate security program.

Physical security measures aim to limit access to authorized personnel, detect unauthorized access, and respond to incidents. Personnel reliability measures help to ensure that the workers who need to handle,

use, and store dangerous materials can be trusted not to conduct a malicious act. Material control and accountability (MC&A) establishes points of responsibility for dangerous materials and creates procedures that track the storage and use of the agents. Transfer security endeavors to provide a measure of security to biological agents outside of access-controlled areas. Information security establishes prudent policies for handling sensitive information associated with the biosecurity program. And program management oversees the development and implementation of an effective biosecurity program. Any biosecurity program should not unduly hinder the normal operations of the bioscience facility. While biosecurity measures may introduce some level of inconvenience into the existing work environment, they must yield benefits in security, personnel safety, and material control and accountability.

Table 1. Example of a Graded Implementation of Biosecurity

	Physical	Personnel	MC&A	Transfer	Information	Program
LRPT	Locked doors – especially when lab is unattended.	Verification of employment history / education background. Guests allowed w/ PI approval.	Laboratory records (e.g. lab notebooks).	PI should be aware of all transfers. Transfers should be documented in lab records.	Prudent policies regarding network security, passwords, email use.	PI ensures that the lab meets all of the recommendations.
MRPT	Access controls that provide reasonable assurance only authorized personnel enter (e.g. controlled keys).	Basic personnel suitability check. Visitors should be escorted, and visitor logs kept. Temporary workers should be escorted or approved. Badges or, for small groups, knowledge of persons.	Stored & used within an access controlled area. Consistent inventory methodology. Lab notebooks document material use (who/when).	Transfers controlled and documented in inventory records. Use of timely shipping methods. Notification of successful receipt.	Prudent policies regarding security information, network security, passwords, email use.	A facility representative should oversee implementation of appropriate biosecurity, ensure biosecurity training, and conduct self-audits.

Table 1 Continued. Example of a Graded Implementation of Biosecurity

	Physical	Personnel	MC&A	Transfer	Information	Program
HRPT	Electronic access controls and a minimal level of intrusion detection. MOU with local law enforcement.	Background investigation. Visitors must be escorted, and visitor logs kept. Temporary workers must be pre-approved and escorted. Photo badges.	Stored & used in an electronic access controlled area. Secure facility-based inventory practices. Usage logs kept, documenting who & when HRPT are accessed.	Biosecurity Officer must pre-approve all transfers. Chain of Custody during transfer. Transfer documented in inventory records. Use of timely shipping methods. Notification of successful receipt.	Strong policies regarding security information, network security, passwords, email use.	Biosecurity Officer should oversee implementation of appropriate biosecurity, ensure biosecurity training, and conduct self-audits.
ERPT	Multiple-level electronic access controls. Intrusion detection. MOU with local law enforcement. Local guard force.	Comprehensive background investigation. All visitors and temporary workers subject to same checks as workers. Photo badges.	Stored and used in multiple-level electronic access controlled area. Secure facility-based inventory practices. Usage logs kept, documenting who & when ERPT are accessed. Two-person rule for access to stocks.	Biosecurity Officer must pre-approve all transfers. Chain of Custody during transfer. Transfer documented in inventory records. Use of timely shipping methods. Notification of successful receipt.	Strong policies regarding security information, network security, passwords, email use.	Biosecurity Officer should oversee implementation of appropriate biosecurity, ensure biosecurity training, and conduct self-audits.

CONCLUSION

This concept of Biosecurity Levels should be developed and vetted through a collaboration of experts in biological weapons, public and agricultural health, microbiology, and security. Analogous to the widely accepted US Biosafety Levels, the Biosecurity Levels would help federal agencies, such as USDA and NIH, apply uniform criteria to grantees, and could form the basis for standardizing biosecurity internationally. Over time, the microbiological community may view standardized Biosecurity Levels, developed according to an agent-based risk assessment, as providing reasonable control recommendations that are proportional to the security risk. Widely accepted biosecurity standards would help facilitate international collaborations by creating more uniform standards. Since funding to increase security often comes at the expense of research, the Biosecurity Levels would help to appropriately allocate scarce security resources, and ensure that biosecurity systems achieve genuine national security objectives. Most importantly, the Biosecurity Levels would remove the ambiguity of the current regulatory approach and facilitate continued biomedical and bioscience research on those agents and toxins deemed most dangerous to human, animal, and plant health in an appropriately protected environment.

REFERENCES CITED

- ¹ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-55, 107th Congress and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law 107-188, 107th Congress.
- ² U.S. National Academy of Sciences, "Biotechnology research in an age of terrorism: Confronting the 'dual use' dilemma" (National Academies Press, Washington, DC, in press); <http://books.nap.edu/catalog/10827.html>.
- ³ Office of the Inspector General, "Controls over Biological, Chemical, and Radioactive Materials at Institutions Funded by the U.S. Department of Agriculture" (U.S. Department of Agriculture, September 2003), Audit Report No. 50099-14-At; <http://www.usda.gov/oig/webdocs/50099-14-At.pdf>.
- ⁴ *ISIS News*, No. 11/12, October 2001, Institute of Science and Society and Department of Biological Sciences, Open University, United Kingdom (UK). <http://www.i-sis.org.uk/isisnews/i-sisnews11-12.php>; J. Cello, A. V. Paul, and E. Wimmer, "Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template," *Science* 297:5583 (August 9, 2002), pp. 1016-1018.
- ⁵ R. M. Salerno, N. Barnett, and J. Koelm, "Balancing Security and Research at Biomedical and Bioscience Laboratories," *BTR 2003: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism—Proceedings* (Albuquerque, NM: March 2003).
- ⁶ The US General Accounting Office has endorsed a risk management approach for mitigating security threats. See US GAO, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, DC: October 2001). Also see US GAO, *Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center*, GAO-03-847 (Washington, DC: September 2003).
- ⁷ Federal Register, Rules and Regulations, Vol 240, No. 67, 42 CFR Part 73, December 13, 2002 (Department of Health and Human Services, Office of the Inspector General), p. 76895; Federal Register, Rules and Regulations, Vol 240, No. 67, 7 CFR Part 331, 9 CFR Part 121, December 13, 2002 (Department of Agriculture, Animal and Plant Health Inspection Service), p. 76921.
- ⁸ CDC's 8th National Symposium on Biosafety, "Biosafety and Biosecurity: A New Era in Laboratory Science" Session Three: Impact of New Regulations, Atlanta, GA (January 27, 2004).
- ⁹ National Institutes of Health and Centers for Disease Control and Prevention, *Biosafety in Microbiological and Biomedical Laboratories*, fourth edition, May 1999 (<http://bmbi.od.nih.gov/contents.htm>).
- ¹⁰ World Health Organization, Laboratory Biosafety Manual, second edition (revised) (2003), http://www.who.int/csr/resources/publications/biosafety/who_cds_csr_lyo_20034/en/.
- ¹¹ "Public Health Assessment of Potential Biological Terrorism Agents," *Emerging Infectious Diseases* 8:2 (February 2002), p. 225-230.
- ¹² http://web.umn.edu/~microbio/BIO221_1998/M_leprae.html.
- ¹³ <http://www.who.int/lep>.
- ¹⁴ <http://microbes.historique.net/leprae.html>.
- ¹⁵ S. Deresinski, "Coccidioides immitis as a Potential Bioweapon," *Seminars in Respiratory Infections* 18:3 (September 2003), p. 216-219.
- ¹⁶ Health Canada, Population and Public Health Branch, Material and Safety Data Sheet, Office of Laboratory Security, January 2000. (<http://www.hc-sc.gc.ca/pphb-dgsp/msds-ftss/msds40e.html>).
- ¹⁷ D. M. Dixon, "Coccidioides immitis as a Select Agent of bioterrorism," *Journal of Applied Microbiology* 91 (2001), p. 602-605.
- ¹⁸ T. C. Dixon, M. Meselson, J. Guillemin, P. C. Hanna, "Anthrax," *The New England Journal of Medicine* 341 (1999) p. 815-829.
- ¹⁹ T. V. Ingelsby, et. al "Consensus Statement: Anthrax as a Biological Weapon," *Journal of the American Medical Association* 281 (1999) p. 1735-1745.
- ²⁰ D. B. Levin, G. Valadares de Amorim, "Potential for Aerosol Dissemination of Biological Weapons: Lessons from Biological Control of Insects" *Biosecurity and Bioterrorism* 1:1 (2003), p. 37-42.
- ²¹ D. A. Henderson et. al, "Consensus Statement: Smallpox as a biological weapon," *Journal of the American Medical Association* 281 (1999) p. 2129-2137.

-
- ²² R. J. Jackson, A. J. Ramsay, C. D. Christensen, S. Beaton, D. F. Hall, I. A. Ramshaw. "Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox," *Journal of Virology* 75 (2001) p. 1205-1210.
- ²³ Jane's Chem-Bio Web, "News, Genetically Modified Smallpox," <http://www.janes.com> (December 13, 2002).
- ²⁴ G. J. Haper, "Airborne micro-organisms: a survival test of four viruses," *Journal of Hygiene* 59 (1961) p. 479-486.